**International Journal of Electronics,
Communication & Instrumentation Engineering
Research and Development (IJECIERD)
ISSN(P): 2249-684X; ISSN(E): 2249-7951
Vol. 4, Issue 2, Apr 2014, 171-182
© TJPRC Pvt. Ltd.**

# EFFICIENT FPGA IMPLEMENTATION OF A SECURE WIRELESS COMMUNICATION SYSTEM USING BLUETOOTH CONNECTIVITY

**MANOHAR V. WAGH[1], MANISHKUMAR GURJAR[2] & MHD. UMMARUDDIN[3]**

[1]Department of Electronics and Communication, TIT College, Bhopal, Madhya Pradesh, India

[2]Professor, Department of Electronics and Communication, TIT College, Bhopal, Madhya Pradesh, India

[3]Department of Electronics and Telecommunication, SITRC, Nashik, Maharashtra, India

## ABSTRACT

In early days, the data transfer was done by wired media like co-axial cable(s), fiber optic cable(s) etc. The era has gone. Nowadays wired media is replaced by wireless means, for which Bluetooth is the best suited choice.

This project emphasizes that wireless communication system for secured data transfer can be implemented by the Bluetooth connectivity. Bluetooth devices are short range and meant for low power utilization, allowing communication between various devices. The Advanced Encryption Standards (AES) algorithm is used in order to provide the security to the data. This project analyzes the development of fully secured wireless connection terminals on a FPGA where connection is established using Bluetooth technology and an advanced encryption standard (AES-128) for encryption and decryption is used to initialize the secured algorithm for data exchange. The prototyping board equipped with Xilinx Spartan-III-XC3S250E-4PQ208 FPGA device is used for hardware evaluation of system design. For simulation part, Xilinx ISE Design Suite 14.2 is used as the simulation tool and architecture was implemented by Verilog. The proposed system has been validated and demonstrated using the application which involves the encryption and decryption of data and evaluated in terms of resources used and throughput obtained.

**KEYWORDS:** Advanced Encryption Standard (AES), Field Programmable Gate Array (FPGA)

## 1. INTRODUCTION

### 1.1 Wireless Communication Techniques

In earlier few decades, the data transfer was done mainly by two media- Guided media and unguided media. Guided media can also be termed as wired media where medium is very important issue. Few examples of wired media are twisted pair cable(s), co-axial cable(s), fiber optic cable(s) etc. Drawbacks of such wired communication are interference, attenuation and limitations to number of receivers which ultimately causes the more attenuation. The solution to this is the unguided communication where wired media is replaced by wireless means of communication. Unguided media can also be termed as wireless media where bandwidth produced by an antenna is an important issue.

Wireless communication technologies which are in use nowadays are Wi-Fi, Bluetooth, Zig-bee and Dash-7(WSN).

Out of these four, we have used Bluetooth technique for the transmission of the data.

Bluetooth was created by Ericsson in 1994 as a wireless alternative for RS232 data cables. Bluetooth is the wireless communication technology managed by Special Interest Group (SIG) in 1998, to fulfill the demands of Wireless Personal Area Networking (WPAN) [1]. It offers wireless, short distance, point to point and point to multipoint data transfer operating at 2.4 GHz Unlicensed Industrial, Scientific and Medical (ISM) band.

From Figure 1, the Bluetooth protocol stack consists of various layers. Any Bluetooth system must have the basic protocols like a radio, base band, link manager and logic link control block. The modulated bit streams are sent and also received with the help of radio protocol. The operations regarding framing, error control, frame control, error correction and detection, timing packet control etc. are performed by base band protocol. The Link Manger protocol manages states and packets and controls the flow on link. The functions of multiplexing and Segmentation and Re-assembly of larger datagram’s into packets are performed by logical link control protocol.

From figure 1, all the logical links are created, modified and released by using link manager. In addition to that, all the parameters related to the physical links between the devices are updated by link manager which is achieved with the help of Link Management Protocol (LMP).

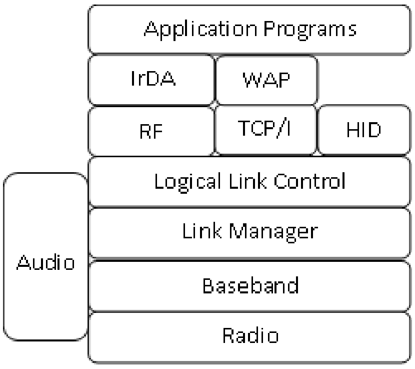

**Figure 1: Bluetooth Protocol Stack [1]**

All the logical links are created, modified and released by using link manager. In addition to that, all the parameters related to the physical links between the devices are updated by link manager which is achieved with the help of Link Management Protocol (LMP). The link controller encodes and decodes the Bluetooth packets from various parameters related to the physical channel [1].

### 1.2 Security for Wireless Communication Techniques

For the purpose of providing security to the data which is transmitted from transmitter to receiver, various secured data transmission techniques are used which protects data from going into the hands of the unauthorized person. Main techniques are – Steganography and Cryptography.

The goal of steganography is to hide messages inside other “harmless” digital media in a way that does not allow any person to even detect the presence of secret message. Steganography does not alter the structure of the secret message, but hides it inside a medium so that the change is not visible. Cryptography hides the contents of a secret message from an unauthorized person but the content of the message is visible. It uses various key based ciphering and deciphering algorithms [2]:-

- **1.2.1 Asymmetric Algorithm:** Uses different key concept.

- **1.2.2 Symmetric Algorithm:** Uses same key concept.

The Symmetric Algorithms are further classified into two main categories [2]:

**Block Ciphers:** In block ciphers, the whole data is divided or organized into the groups or blocks, so it is called as the block ciphers [3].

**Stream Ciphers:** In stream ciphers, instead of grouping the data, only single bit data is sent at a time and so it is operated in real-time manner [4].

There are various Symmetric Block Ciphers

- Data Encryption Standards (DES)[5]
- Triple Data Encryption Standards (T-DES)[5]
- Advanced Encryption Standards (AES)[5]

These three are invented one after another overcoming the drawbacks of previous ones.

So finally, for secure transmission of data, the AES-128 algorithm has been implemented successfully in this paper. Reconfigurable hardware (RH) in the form of field programmable gate arrays (FPGAs) can be an ideal candidate to embed this technology for wireless communication applications. FPGAs are widely used in digital signal processing and communication systems. The advantages offered by FPGAs, such as massive parallelism capabilities, multimillion gate counts, and special low power packages can reduce the amount of memory used, computational complexity and power consumption.

The main aim of this paper is to develop a reconfigurable environment for secure data transfer using Bluetooth connectivity. An efficient implementation of the advanced encryption standards (AES) algorithm has been carried out on the prototyping board equipped with Spartan 3 FPGA chip. The rest of the paper is organized as follows. The implemented system architecture is presented in section 2.The FPGA implementation is described in section 3. Results and analysis are presented in section 4.Concluding remarks are given in Section 5.

## 2. IMPLEMENTED SYSTEM

FPGA processes the acquired data and operates as the base station of the transferred data. The prototyping board has been used for testing and evaluating the implemented system. It is equipped with the Xilinx Spartan-III-XC3S250E-4PQ208 FPGA chip. Bluetooth connection has been established using the Bluetooth Module-HC-O5 on both transmitting and receiving terminals. At the receiving section, the data is decrypted using decryption algorithm. This section describes the implementation of the hardware set-up needed for the execution of the implemented work along with the details of each hardware component required to build the whole system in its initial part. Later part describes the simulation results obtained using Xilinx 14.2

Figure 2 Shows the Implemented System with its main building blocks

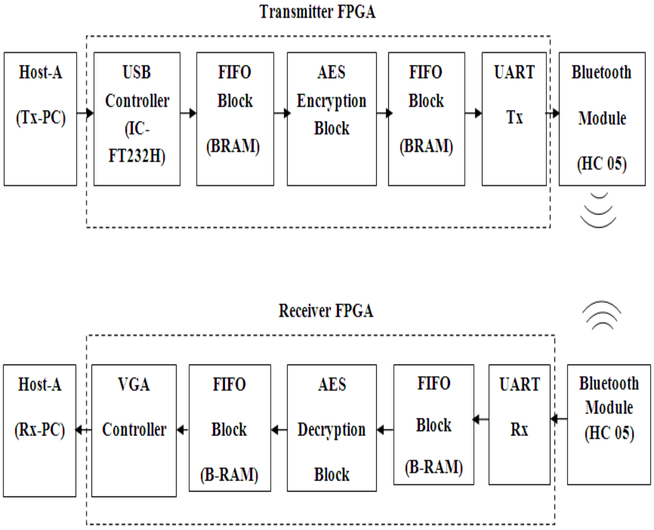

**Figure 2: Block Diagram of Implemented System**

The transmitter block obtains its data which can be numbers, text or images through Host PC-A. The USB controller maintains the connection with the external environment and controls host PC. It requires 12 MHz oscillator whose output is given to USB and FPGA chip. The IC FT232H is a single channel USB 2.0 Hi-Speed (480Mb/s) to UART/FIFO IC. Then picoblaze which is 8-bit soft core reconfigurable controller is implemented on the Spartan-III. Here two picoblaze controllers are used at the transmitter section and two more are used at the receiver section of FPGA. The size of one B-RAM is 2048 bytes. So if the size of an image is increased, then number of B-RAM is increased. This FIFO block is used to match the speed of the two devices attached on both the sides. In our project, the maximum storage capacity of FIFO block is 15000 bytes. So if any image more than 15000 bytes is taken for the transmission purpose then overwriting of data will take place. Then AES algorithm is used to transmit the data securely using Bluetooth connectivity to the receiver block.

## 3. SYSTEM IMPLEMENTATION

The first step of the implementation is concerned with the development of a Bluetooth connection between two boards; then followed by AES algorithm implementation (AES-128). Figure 3 shows the implemented reconfigurable environment using FPGA and Bluetooth connectivity. Verilog programming language has been used for hardware compilation and efficient implementation of different tasks and algorithms.

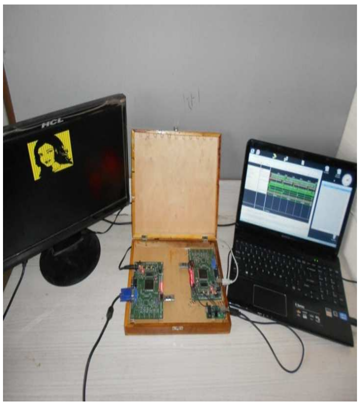

**Figure 3: FPGA Boards Communicating via Bluetooth**

## A. Encryption Algorithm

The AES algorithm consists of ten rounds of encryption and each round includes four transformations using the corresponding cipher key to ensure the security of the encryption. Output of one round is forwarded to next round and after final round; the cipher text is available which the output of encryption process is. Each of the four transformations has certain uniqueness in their operation [6].

These four transformations are given as follows:

- Sub Bytes (),
- Shift Rows (),
- Mix Columns (),
- Add Round Key ().

**Table 1: Round Functions for Encryption Process**

| Round | Function |
|---|---|
| - | Add Round Key(State) |
| 0 | Add Round Key(Mix Column(Shift Row(Byte Sub(State)))) |
| 1 | Add Round Key(Mix Column(Shift Row(Byte Sub(State)))) |
| 2 | Add Round Key(Mix Column(Shift Row(Byte Sub(State)))) |
| 3 | Add Round Key(Mix Column(Shift Row(Byte Sub(State)))) |
| 4 | Add Round Key(Mix Column(Shift Row(Byte Sub(State)))) |
| 5 | Add Round Key(Mix Column(Shift Row(Byte Sub(State)))) |
| 6 | Add Round Key(Mix Column(Shift Row(Byte Sub(State)))) |
| 7 | Add Round Key(Mix Column(Shift Row(Byte Sub(State)))) |
| 8 | Add Round Key(Mix Column(Shift Row(Byte Sub(State)))) |
| 9 | Add Round Key(Shift Row(Byte Sub(State))) |

The key expansion processed at the same time with the AES transformations, in order to conserve the clock cycle which is called the Pipelined method [7]. Figure 4 shows the transmitter encryption algorithm.

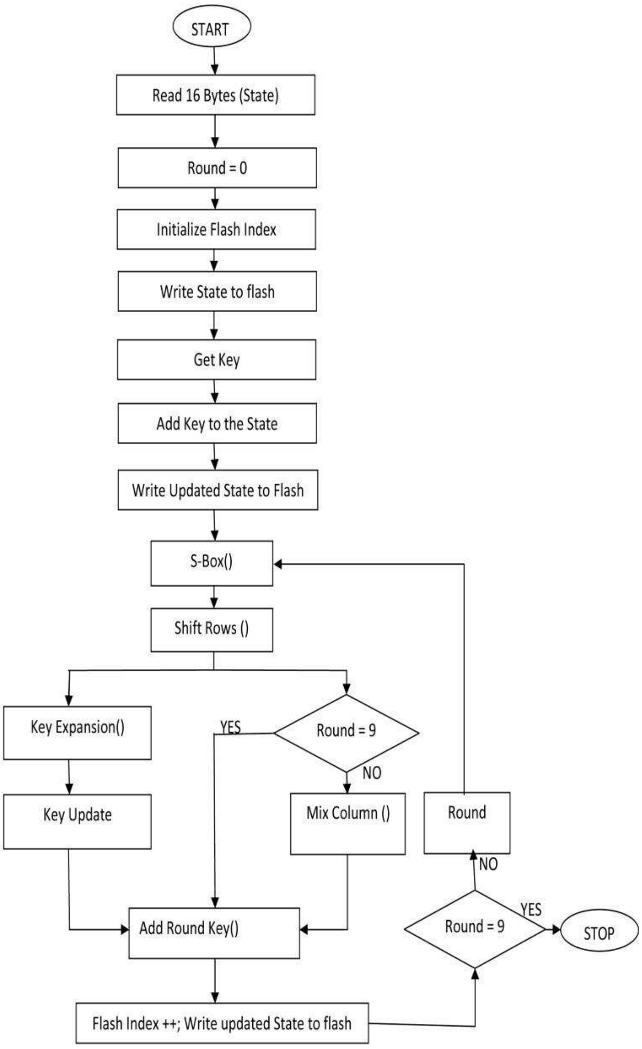

**Figure 4: Encryption Algorithm [8]**

### B. Decryption Algorithm

Decryption process is the exactly reverse process of the encryption process. The stream of 15000 bytes cipher text is received in the receiver block via wireless communication media. and after reception at the receiver section, the data i.e.

Cipher text undergoes decryption process. All the transformations in decryption algorithm are executed one after another and the output of first round is forwarded to the next round in the form of input and finally after the last round, final plaintext is available which are the output of decryption process and the exact similar input of encryption process. Each of the four transformations has certain uniqueness in their operation

Again the data received at the receiver block undergoes four operations-

- Inverse Shift Rows(),
- Inverse Sub-Bytes(),
- Inverse Add Round Key ().
- Inverse Mix Columns.

**Table 2: Round Functions for Decryption Process**

| Round | Function |
|---|---|
| - | Add Round Key(State) |
| 9 | Mix Column(Add Round Key(Byte Sub(Shift Row(State)))) |
| 8 | Mix Column(Add Round Key(Byte Sub(Shift Row(State)))) |
| 7 | Mix Column(Add Round Key(Byte Sub(Shift Row(State)))) |
| 6 | Mix Column(Add Round Key(Byte Sub(Shift Row(State)))) |
| 5 | Mix Column(Add Round Key(Byte Sub(Shift Row(State)))) |
| 4 | Mix Column(Add Round Key(Byte Sub(Shift Row(State)))) |
| 3 | Mix Column(Add Round Key(Byte Sub(Shift Row(State)))) |
| 2 | Mix Column(Add Round Key(Byte Sub(Shift Row(State)))) |
| 1 | Mix Column(Add Round Key(Byte Sub(Shift Row(State)))) |
| 0 | Add Round Key(Byte Sub(Shift Row(State))) |

The following Figure 5 shows the decryption design flow with unpipelined method [8].

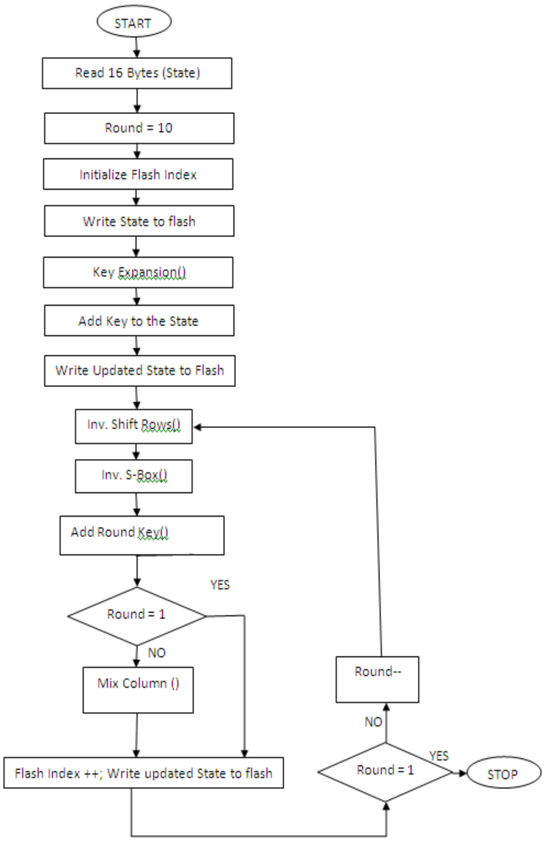

**Figure 5: Decryption Algorithm [8]**

The following tables show the resource utilization at the transmitter and receiver respectively.

**Table 3: Resources Used for System at Transmitter**

| Logic Utilization | Used | Available | Utilization |
|---|---|---|---|
| No. of Slice Flip Flops | 784 | 4896 | 16% |
| Number of 4-input LUTs | 4469 | 4896 | 91% |
| **Logic Distribution** | | | |
| Number of occupied Slices | 2386 | 2448 | 97% |
| Slice containing only related logic | 2386 | 2386 | 100% |
| Number of slice containing unrelated logic | 0 | 2386 | 0% |

**Table 3: Contd.,**

| | | | |
|---|---|---|---|
| **Total number of 4-input LUTs** | 4558 | 4896 | 93% |
| Number used as logic | 4297 | - | - |
| Number used as route-through | 89 | - | - |
| Number used for dual port RAMs | 32 | - | - |
| Number used for 32*1 RAMs | 104 | - | - |
| Number used as Shift Registers | 36 | - | - |
| **Bonded IOBs** | 45 | 158 | 28% |
| **IOB Flip Flops** | 33 | - | - |
| **RAMB 16s** | 11 | 12 | 91% |
| **BUFGMUXs** | 6 | 64 | 25% |
| **DCMs** | 1 | 4 | 25% |

**Table 4: Resources Used for System at Receiver**

| Logic Utilization | Used | Available | Utilization |
|---|---|---|---|
| No. of Slices | 467 | 2448 | 19% |
| Number of Slice Flip-Flops | 539 | 4896 | 11% |
| Number of 4-input LUTs | 757 | 4896 | 15% |
| Number of bonded IOBs | 45 | 158 | 28% |
| Number of TBUFs | 2 | 0 | - |
| Number of BRAMs | 10 | 12 | 83% |
| Number of GCLKs | 6 | 24 | 25% |
| Number of DCMs | 1 | 4 | 25% |

## 4. RESULTS AND ANALYSIS

After implementing the whole system on the FPGA boards, various types of data like simple text, black and white images and coloured images were transmitted from the transmitter FPGA to the receiver FPGA via bluetooth module.

The results of encryption and decryption of few blocks are mentioned below along with the initial cipher key. The same key is used hare for the encryption and decryption process as it is the symmetric key cryptographic algorithm.

**Outputs of some sample test vectors of encryption-decryption algorithms for verification**

**Cipher Key**=2b7e151628aed2a6abf7158809cf4f3c

**Block-1**

A) **For Encryption**

Plaintext----FC00017E1FFFFFE00020C00000080093

Cipher text----4b4d4cb825b019757778b2655016e39c

B) **For Decryption**

Cipher text-----4b4d4cb825b019757778b2655016e39c

Plaintext-----FC00017E1FFFFFE00020C00000080093

**Block-2**

A) **For Encryption**

Plaintext---- 03FFFFF0200038008000005917FFFFFFCipher text----0bd286faff623e4bf9a79b1e4407b263

**B) For Decryption**

Cipher text-----0bd286faff623e4bf9a79b1e4407b263

Plaintext----- 03FFFFF0200038008000005917FFFFFF

**Block-3**

**A) For Encryption**

Plaintext----01FFFFC0001F01FFFFFF2BFFE0080000Cipher text----5ebd629c037247199c75bd6f484688cb

**B) For Decryption**

Cipher text-----5ebd629c037247199c75bd6f484688cb

Plaintext----01FFFFC0001F01FFFFFF2BFFE0080000

**Block-4**

**A) For Encryption**

Plaintext---01FFFF800003803FFFC07F0FFE0C8000 Cipher text----4c6cbee09c07e474d4e31f541961a96a

**B) For Decryption**

Cipher text-----4c6cbee09c07e474d4e31f541961a96a

Plaintext----01FFFF800003803FFFC07F0FFE0C8000

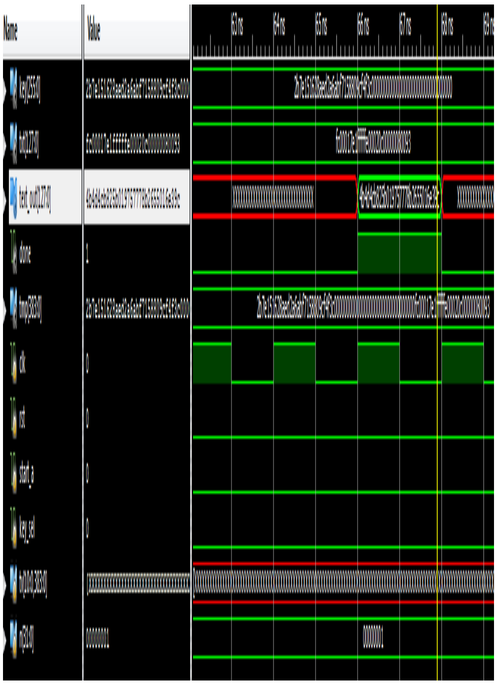

**Figure 6: Encryption Process Screenshot**

Above figure shows the encryption of first block of test samples. Similarly other blocks were considered for the decryption process and its simulation output is as follows,

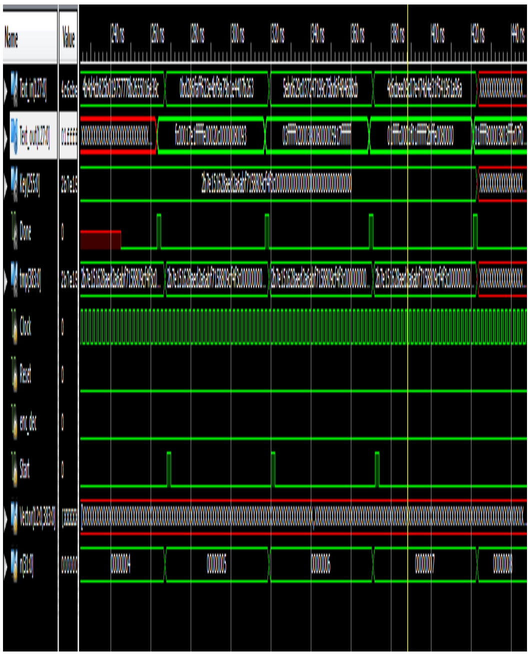

**Figure 7: Decryption Process Screenshot**

**Table 5: Comparison of Implemented System with Other Existing Systems [7]**

| Design | Device | Slice | Block RAM | Max Frq.(MHz) | Throughput (Gbit/s) | Throughput/Slice (Mbps/Slice) |
|---|---|---|---|---|---|---|
| Proposed System | SpartanIII-XC3S250E-4 | 467 | 10 | 89.98 | 0.216 | 0.4 |
| Has an Tasha, et al.[7] | Spartan-III XC3S15001 | 2,564 | N/A | 61.5 | 7.9 | 3.2 |
| Rouvroy et al.[9] | Spartan-III XC3S50-4 | 163 | 3 | 71 | 0.208 | 0.13 |
| Chodowiec & Gaj [10] | Spartan-II XC2S30-6 | 222 | 3 | 60 | 0.166 | 0.07 |
| Zambreno et al. [11] | Virtex-II XC2V4000 | 16,938 | N/A | 184.1 | 23.654 | 1.39 |
| Qin et al. [12] | Altera stratix 1S20C5 | 5,145 | N/A | 39.68 | 5.61 | 1.12 |
| Jarvinen et al. [13] | Virtex-E XCv1000e-8 | 5,810 | 100 | 158 | 20.3 | 1.09 |
| Standaert et al. [14] | Virtex-E XCV 3200e-8 | 9,446 | N/A | 169.1 | 21.64 | 2.29 |
| Saggesse et al. [15] | Virtex-E XCV 2000e-8 | 11,719 | N/A | 129.2 | 16.5 | 1.48 |
| Hodjat & verbauwhede [16] | Virtex-II Pro-XC2VP20 | 15,112 | N/A | 145 | 18.56 | 1.22 |

## 5. CONCLUSIONS

AES-128 bit algorithm has been implemented successfully in this paper for secure data transmission between two terminals. The prototyping boards have been used to demonstrate and validate the system. The system has been evaluated and compared with existing implementations. It shows better results in terms of overall system throughput rate and throughput per slice rate with decrease in chip area thus thereby reducing overall power consumption.

## REFERENCES

1. Etienne van der Lindeand Gerhard P. Hancke, “An Investigation of Bluetooth Mergence with Ultra Wideband”, At third International Conference on Broadband Communications, Information Technology & Biomedical Applications, 978-0-7695-3453-4/08-2008, DOI-10.11.09/BROADCOM.22. PP. 451-457, IEEE 2008.

2. Naif A. Kofahi, Turki Al-Somani and Khalid Al-Zamil, “Performance Evaluation of Three Encryption/Decryption Algorithms”, At 46th Midwest Symposium on Circuits and Systems,2004, on 30 Dec.2004, Volume-2, PP 790-793 ISSN- 0-7803-8294-3/04/2004, IEEE 2004.

3. S. Goldwasser and S. Micali, "Probabilistic Encryption", Journal of Computer And System Sciences, vol 28, PP 270-299, 1994.

4. M.J.B. Robs Haw, “Stream Ciphers” Technical Report, RSA Data Security, Inc., Number TR-701, PP 46, July 1995.

5. Mamta Sood, Manohar Wagh, Monika Cheema, “A Review on Various Data Security Techniques in Wireless Communication System”, At International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 3, Issue 2, pp.883-890, March -April 2013,

6. Gohil Rikitaben Karsanbhai, and Mary Grace Shajan, “128 Bit AES Implementation for Secured Wireless Communication”, 978-1-4577-0240-2/11/ PP-497-501, IEEE 2011.

7. Hasasn Taha, Abdul N. Sazish, Afandi Ahmead, Mhd. Saeed Sharif And Abbes Amira, “Efficient FPGA Implementation of A Wireless Communication System Using Bluetooth Connectivity “, 2010, PP. 1767-1770, IEEE 2010.

8. Anurag Gupta, Afandi Ahmadd, Mhd Saeed Sharif And Abbes Amira, “Rapid Prototyping Of AES Encryption for Wireless Communication System On FPGA”. At IEEE 15th International Symposium on Consumer Electronics, 978-1-61284-843-3 on 14-17 June 2011, ISSN 0747-668X, IEEE 2011.

9. G. Rouvroy, F-X Standard, J.-J. Quisquater, And J.-D. Legat, “Compact And Efficient Encryption/ Decryption Module For FPGA Implementation of The AES Rijndael Very Well Suited for Small Embedded Applications”, At Information Technology: Coding And Computing, 2004.V. Proceedings. ITCC 2004, International Conference On, Volume 2, PP 583-587. April 2004.

10. Pawel Chodoweic and Kris Gaj, “Very Compact FPGA Implementation Of AES Algorithm”, Cryptographic Hardware And Embedded Systems-CHES -2003, 2779:319-333, Oct. 2003.

11. Joseph Zambreno, David Nguyen and Alok Chaudhary, “Exploring Area/ Delay Tradeoffs In An AES FPGA Implementation”, At Proceedings of The 14 The Annual International Conference on Field Programmable Logic And Applications, In FPL 04, PP 575-585, Springer 2004.

12. Hui Qin, Tsutomu Sasao and Yukihiro Iguchi. “An FPGA Design of AES Encryption Circuit with 128-Bit Keys”, At GLSVLSI '05: Proceedings of The 15th ACM Great Lakes Symposium On VLSI, PP 147-151, 2005.

13. Kimmo U. Jarvinen, Matti T. Tommiska, and Jorma O. Skytta, “A Fully Pipelined Memory less 17.8 GBPS AES-128 Encryptor”, At FPGA '03: Proceedings of The 2003 ACM/CIGDA Eleventh International Symposium On Field Programmable Gate Arrays, PP 207-215, New York, NY, USA, ACM ,2003.
14. Francois-Xavier Standaert, Gael Rouvroy, Jean- Jacques Quisquater And Jean Didier Legat, “Efficient Implementation Of Rijndael Encryption In Reconfigurable Hardware And Embedded Systems”, At CHES 2003, PP 334-350, May 2003.
15. Giacinto Paolo Saggase, Antonino Mazzeo, Nicola Mazzocca And Antonio G.M. Strollo, “An FPGA- Based Performance of The Unrolling, Tiling And Pipelining of The AES-Algorithm”. At FPL, PP 292-302, 2003.
16. Hodjat And I. Verbauwhede, “A 21.54 GBPS Fully Pipelined AES Processor On FPGA”, At Field Programmable Custom Computing Machines, 2004 (FCCM 2004), 12th Annual IEEE Symposium, PP 308-309, April’04, IEEE 2004.